Theoretical Computer Science 598 (2015) 129–137

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

On weak odd domination and graph-based quantum secret sharing

Sylvain Gravier [a,b], Jérôme Javelle [b,c,*], Mehdi Mhalla [a,c], Simon Perdrix [a,c]

[a] *CNRS, France*
[b] *Université de Grenoble, France*
[c] *Laboratoire d'Informatique de Grenoble, France*

ARTICLE INFO

Article history:
Received 30 January 2013
Received in revised form 25 May 2015
Accepted 26 May 2015
Available online 29 May 2015
Communicated by L. Kari

Keywords:
Complexity
Graph theory
NP-completeness
Quantum information

ABSTRACT

A weak odd dominated (WOD) set in a graph is a subset B of vertices for which there exists a distinct set of vertices C such that every vertex in B has an odd number of neighbors in C. We point out the connections of weak odd domination with odd domination, $[\sigma, \rho]$-domination, and perfect codes. We introduce bounds on $\kappa(G)$, the maximum size of WOD sets of a graph G, and on $\kappa'(G)$, the minimum size of non-WOD sets of G. Moreover, we prove that the corresponding decision problems are NP-complete.

The study of weak odd domination is mainly motivated by the design of graph-based quantum secret sharing protocols: a graph G of order n corresponds to a secret sharing protocol whose threshold is $\kappa_Q(G) = \max(\kappa(G), n - \kappa'(G))$. These graph-based protocols are very promising in terms of physical implementation, however all such graph-based protocols studied in the literature have quasi-unanimity thresholds (i.e. $\kappa_Q(G) = n - o(n)$ where n is the order of the graph G underlying the protocol). In this paper, we show using probabilistic methods the existence of graphs with smaller κ_Q (i.e. $\kappa_Q(G) \le 0.811n$ where n is the order of G). We also prove that deciding for a given graph G whether $\kappa_Q(G) \le k$ is NP-complete, which means that one cannot efficiently double check that a graph randomly generated has actually a κ_Q smaller than $0.811n$.

1. Introduction

1.1. Odd domination

Odd domination is a variant of domination in which, given a graph $G = (V, E)$, a set $C \subseteq V$ oddly dominates its closed odd neighborhood $Odd[C] := \triangle_{v\in C} N[v] = \{u \in V, |N[u] \cap C| = 1 \bmod 2\}$ defined as the symmetric difference of the closed neighborhoods $N[v] = \{v\} \cup N(v)$ of the vertices v in C, where $N(v) = \{u \in V, (u, v) \in E\}$ is the (open) neighborhood of v. An odd dominating set is a set of vertices $C \subseteq V$ such that $Odd[C] = V$. Odd dominating sets have been largely studied in the literature [1,4] in particular for their role in the sigma-game [26,25]. It has been noticeably proven that every graph contains at least one odd-dominating set [26] and that deciding whether a graph contains an odd dominating set of size at most k is NP-complete [26].

[*] Corresponding author.
E-mail address: jerome.javelle@imag.fr (J. Javelle).

http://dx.doi.org/10.1016/j.tcs.2015.05.038
0304-3975/© 2015 Elsevier B.V. All rights reserved.

Odd domination is a particular instance of the general framework of $[\sigma,\rho]$-domination [8,27]. Given $\sigma,\rho \subseteq \mathbb{N}$, a $[\sigma,\rho]$-dominating set in a graph $G=(V,E)$ is a set $C \subseteq V$ such that $\forall v \in C, |N(v)\cap C| \in \sigma$, and $\forall v \in V \setminus C$, $|N(v)\cap C| \in \rho$. Among others, domination, independent set, perfect code, and odd domination problems can be formulated as $[\sigma,\rho]$-domination problems. In particular, odd domination corresponds to [EVEN, ODD]-domination,[1] where EVEN $=\{2n, n\in\mathbb{N}\}$ and ODD $=\mathbb{N}\setminus$ EVEN. The role of the parameters σ and ρ in the computational complexity of the corresponding decision problems have been studied in the literature [27].

We consider a weaker version of odd domination which does not fall within the $[\sigma,\rho]$-domination framework. A weak odd dominated (WOD) set is a set $B \subseteq V$ for which there exists $C \subseteq V \setminus B$ such that $B \subseteq Odd[C]$. Notice that, since $B\cap C=\emptyset$, $B \subseteq Odd[C]$ if and only if $B \subseteq Odd(C) := \Delta_{v\in C} N(v) = \{u \in V, |N(u)\cap C| = 1 \mod 2\}$. Roughly speaking, B is a weak odd dominated set if it is oddly dominated by a set C which does not intersect B. Weak odd domination does not fall within the $[\sigma,\rho]$-domination framework because, intuitively, a weak odd dominated set is not oddly dominated by its complementary set (as it would be in the $[\mathbb{N}, \text{ODD}]$-domination) but by a subset of its complementary set.

We consider two natural optimization problems related to weak odd dominated sets of a given graph G: finding the size $\kappa(G)$ of the greatest WOD set and finding the size $\kappa'(G)$ of the smallest set which is not a WOD set. The greatest WOD set has a simple interpretation in a variant of the sigma-game: given a graph G, each vertex has three possible states: 'on', 'off', and 'broken'; when one plays on a vertex v, it makes the vertex v 'broken' and flips the states 'on'/'off' of its neighbors. In the initial configuration all vertices are 'off'. The size $\kappa(G)$ of the greatest WOD set corresponds to the greatest number of (unbroken) 'on' vertices one can obtain.

In Section 2, we illustrate the weak odd domination by the computation of κ and κ' on a particular family of graphs. Moreover, we give non-trivial bounds on these quantities, and show that the corresponding decision problems are NP-complete.

1.2. Graph-based quantum secret sharing

Our main motivation for studying weak odd dominated sets is not the variant of the sigma-game but their crucial role in graph-based protocols for quantum secret sharing. A quantum secret sharing scheme [6] consists in sharing a quantum state among n players such that authorized sets of players can reconstruct the secret. The protocol admits a threshold k if any set of at least k players can reconstruct the secret whereas any set of less than $k-1$ players has no information about the secret. Notice that a direct consequence of the no-cloning theorem [30] is that the threshold of any quantum secret sharing protocol on n players must be greater than $n/2$.

In a graph-based quantum secret sharing [17,11] the quantum state shared by the players is characterized by a simple undirected graph. In Section 3, we show that the threshold of such a quantum secret sharing protocol based on a graph G of order n is $\kappa_Q(G)+1$, where $\kappa_Q(G)=\max(\kappa(G), n-\kappa'(G))$. Graph-based quantum secret sharing are very promising in terms of physical implementation [21,29], however all the known graph-based secret sharing protocols have a threshold $n-o(n)$ (the best known protocol has a threshold $n-n^{0.68}$ [11]), where n is the number of players. On the other hand, it has been proved that the threshold of any graph-based quantum secret sharing protocol on n players is at least $\frac{n}{2}+\frac{n}{156}$ [11].

In Section 4, we prove that there exists a family $\{G_i\}$ of graphs such $\kappa_Q(G_i) \le 0.811n_i$ where n_i is the order of G_i. It crucially shows that graph-based quantum secret sharing protocols are not restricted to quasi-unanimity thresholds. We actually prove that almost all the graphs have such a 'small' κ_Q: if one picks a random a graph G of order n (every edge occurs with probability 1/2), then $\kappa_Q(G) \le 0.811n$ with probability greater than $1-\frac{1}{n}$. We also prove that, given a graph G and a parameter k, deciding whether $\kappa_Q(G) \ge k$ is NP-complete. As a consequence, one cannot efficiently verify that a particular randomly generated graph has actually a 'small' κ_Q.

1.3. Combinatorial properties of graph states

The development and the study of graph-based protocols [17,13,11,23,10] have already pointed out deep connections between graph theory and quantum information theory. For instance, it has been shown [12] that a particular notion of flow [5,2,19,18] in the underlying graph captures the flow, during the protocol, of the information contained in the secret from the dealer – who encodes the secret and sends the shares – to the authorized sets of players. The results presented in this paper contribute to these deep connections: we show that weak odd domination is a key concept for studying the properties of graph-based quantum secret sharing protocols.

The study of graph-based protocols also contributes, as a by-product, to a better understanding of the combinatorial properties of a particular class of quantum states, called graph states [9]. The graph state formalism is a very powerful tool which is used in several areas of quantum information processing. Graph states provide a universal resource for quantum computing [22,28] and are also used in quantum correction codes [24,3] for instance. Moreover, they are very promising in terms of physical implementation [21,29]. As a consequence, progresses in the knowledge of the fundamental properties of graph states can potentially impact not only quantum secret sharing but a wide area of quantum information processing.

[1] Notice that odd domination is not a [ODD, ODD]-domination because open neighborhood are considered in the $[\sigma,\rho]$-domination instead of the closed neighborhood in the odd domination.